

Dataskyddsförordningen (GDPR)

25 maj 2018

General Data Protection Regulation

Syften

- Skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, dvs **ökad integritet för personer**
- skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter inom EU så att det fria flödet av uppgifter inom unionen inte hindras, dvs **smidigare för företag att flytta verksamhet inom EU**

Vad skiljer GDPR från Pul?

- **Stärkta rättigheter.** Rätt att få information om sin registrering och att bli "bortglömd" eller uppgifter rättas.
- **Stärkta krav på samtycke**
- **Förtydligt och utökat ansvar för personuppgiftsansvariga och personuppgiftsbiträden**
- **Strängare sanktioner** – effektiva, proportionella och avskräckande
- **Skyldighet att anmäla och informera** om personuppgiftsincidenter

Personuppgiftsansvariga= den juridiska personen som bestämmer ändamål och medel för personuppgifternas hantering. Dvs varför och hur.

Personuppgiftsbiträden, är den som behandlar personuppgifter för den ansvariges räkning. *OBS! Alltid utanför den egna organisationen.*

Principer för GDPR

NYTT!

Principerna för att få lagra personuppgifter:

- Det måste finnas en laglig grund: Text samtycke, avtal, intresseavvägning
- Integritet och konfidentialitet – Högra krav på säkerhet
- Ansvarsskyldighet – Dokumentation!
- Personuppgifter inte längre en särfråga – Fler får ansvar för hanteringen.

Kvar sedan tidigare enligt Pul

- Ändamålsbegränsning – Informera om ändamålet!
- Uppgiftsminimering – Ingen lagring för säkerhetsskull!
- Korrekthet – Rätt uppgifter.
- Lagringsminimering – Inte längre än nödvändigt. Motiverar att man sparar.

Man måste ha laglig grund för att spara personuppgifter

Fyra vanlig grunder:

- Samtycke – tex vid känsliga uppgifter
- Avtal – tex myndigheter
- Intresseavvägning – tex marknadsföring (medlemsförteckning), vetenskaplig eller historisk forskning, allmänintresse
- Rättslig förpliktelse – tex bokföringslagen

Tänk på att ...

- Var noga med att informera personer om varför ni sparar deras personuppgifter, tex när en person blir medlem i en förening.
- Spara aldrig information om ni inte har anledning!
- Se till att ha ordning på samtycken, om ni samlar in sådana.
- En person har alltid rätt att få information om vilka personuppgifter som lagrats. Det gäller även information som förekommer i mailväxlingar.
- En person har rätt att bli "bortglömd", dvs borttagen från register.
- En förening har å sin sida rätt att spara personuppgifter för att kunna kontakta sina medlemmar. Att kräva personnummer är sällan nödvändigt och kräver därför extra starkt motiv.
- Finns det externa företag eller föreningar utanför föreningen som hanterar de personuppgifter som ni samlar in? I så fall behöver ni skriva ett personuppgiftsbiträdesavtal (PUBA).

GDPR – artikel 30

register över behandling

- Personuppgiftsansvarig skall föra register över åtgärder innehållande:
 - Namn och kontaktuppgift på personuppgiftsansvarig och dennes företrädare
 - Ändamål med registret
 - Vilka som får ta del av registret
 - När uppgifter raderas
- På uppmaning göra registret tillgängligt för tillsyningsmyndighet

Läs mer om GDPR på www.datainspektionen.se

Exempel

Medlemsförteckning Lunda hbf

- Personuppgiftsansvarig: Ordf Karl Karlsson tfn 070- ... samt föreningens kassör Snål Jåp tfn xxxx
- Medlemsregister för kontakt med medlemmar i Lunda hbf
- Registret är tillgängligt för föreningens styrelse och valberedning
- Översyn sker varje år varvid utgångna medlemmar tas bort

Sammanfattning

- Informera medlemmarna att de finns i medlemsförteckningen och ev. andra listor
- Informera om vad som finns i registret och varför
- Håll förteckningarna/registren aktuella och för logg över förändringar (åtgärder)
- Upprätta lista på vilka register/lister föreningen för (glöm inte e-postlistan, värddar på hembygdsgården osv)
- Aldrig lämna ut registret

www.datainspektionen.se